Exhibit B

Department of Justice

U.S. Attorney's Office

Southern District of New York

FOR IMMEDIATE RELEASE Wednesday, December 1, 2021

Former Employee Of Technology Company Charged With Stealing Confidential Data And Extorting Company For Ransom While Posing As Anonymous Attacker

Damian Williams, the United States Attorney for the Southern District of New York, and Michael J. Driscoll, Assistant Director-in-Charge of the New York Office of the Federal Bureau of Investigation ("FBI"), announced the arrest today of NICKOLAS SHARP for secretly stealing gigabytes of confidential files from a New York-based technology company where he was employed ("Company-1"), and then, while purportedly working to remediate the security breach, extorting the company for nearly $2 million for the return of the files and the identification of a remaining purported vulnerability. SHARP subsequently re-victimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated, which were followed by a significant drop in the company's share price associated with the loss of billions of dollars in its market capitalization.

SHARP was arrested earlier today in the District of Oregon and will be presented this afternoon before U.S. Magistrate Judge John V. Acosta. The case was assigned to U.S. District Judge Katherine Polk Failla.

U.S. Attorney Damian Williams said: "As alleged, Nickolas Sharp exploited his access as a trusted insider to steal gigabytes of confidential data from his employer, then, posing as an anonymous hacker, sent the company a nearly $2 million ransom demand. As further alleged, after the FBI searched his home in connection with the theft, Sharp, now posing as an anonymous company whistle-blower, planted damaging news stories falsely claiming the theft had been by a hacker enabled by a vulnerability in the company's computer systems. Now the alleged theft and lies have been exposed, and Sharp is facing serious federal charges."

FBI Assistant Director Michael J. Driscoll said: "We allege Mr. Sharp created a twisted plot to extort the company he worked for by using its technology and data against it. Not only did he allegedly break several federal laws, he orchestrated releasing information to media when his ransom demands weren't met. When confronted, he then lied to FBI agents. Mr. Sharp may have believed he was smart enough to pull off his plan, but a simple technical glitch ended his dreams of striking it rich."

According to the Indictment unsealed today in Manhattan federal court[1]:

At all times relevant to the Indictment, Company-1 was a technology company headquartered in New York that manufactured and sold wireless communications products, and whose shares were traded on the New York Stock Exchange. NICKOLAS SHARP, the defendant, was employed by Company-1 from in or about August 2018 up to and including on or about April 1, 2021. SHARP was a senior developer who had access to credentials for Company-1's Amazon Web Services ("AWS") and GitHub Inc. ("GitHub") servers.

In about December 2020, SHARP repeatedly misused his administrative access to download gigabytes of confidential data from his employer. For the majority of this cybersecurity incident (the "Incident"), SHARP used a virtual private network service that he subscribed to from a company named Surfshark to mask his Internet Protocol ("IP") address when he accessed Company-1's AWS and GitHub infrastructure without authorization. At one point during the exfiltration of Company-1 data, SHARP's home IP address became unmasked following a temporary internet outage at SHARP's home.

During the course of the Incident, SHARP caused damage to Company-1's computer systems by altering log retention policies and other files, to conceal his unauthorized activity on the network. In or about January 2021, while working on a team remediating the effects of the Incident, SHARP sent a ransom note to Company-1, posing as an anonymous attacker who claimed to have obtained unauthorized access to Company-1's computer networks. The ransom note sought 50 Bitcoin, a cryptocurrency – which was the equivalent of approximately $1.9 million, based on the prevailing exchange rate at the time – in exchange for the return of the stolen data and the identification of a purported "backdoor," or vulnerability, to Company-1's computer systems. After Company-1 refused the demand, SHARP published a portion of the stolen files on a publicly accessible online platform.

On or about March 24, 2021, FBI agents executed a search warrant at SHARP's residence in Portland, Oregon, and seized certain electronic devices belonging to SHARP. During the execution of that search, SHARP made numerous false statements to FBI agents, including, among other things, in substance, that he was not the perpetrator of the Incident and that he had not used Surfshark VPN prior to the discovery of the Incident. When confronted with records demonstrating that SHARP purchased the Surfshark VPN service in July 2020, approximately six months prior to the Incident, SHARP falsely stated, in part and substance, that someone else must have used his PayPal account to make the purchase.

Several days after the FBI executed the search warrant at SHARP's residence, SHARP caused false news stories to be published about the Incident and Company-1's response to the Incident and related disclosures. In those stories, SHARP identified himself as an anonymous whistleblower within Company-1 who had worked on remediating the Incident. In particular, SHARP falsely claimed that Company-1 had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to Company-1's AWS accounts. In fact, as SHARP well knew, SHARP had taken Company-1's data using credentials to which he had access in his role as Company-1's AWS cloud administrator, and SHARP had used that data in a failed attempt to extort Company-1 for millions of dollars.

Following the publication of these articles, between March 30, 2021, and March 31, 2021, Company-1's stock price fell approximately 20%, losing over $4 billion in market capitalization.

SHARP, 36, of Portland, Oregon, is charged in four counts. The first count charges him with transmitting a program to a protected computer that intentionally caused damage, which carries a maximum sentence of 10 years in prison. The second count charges transmission of an interstate threat, which carries a maximum sentence of two years in prison. The third count charges wire fraud, which carries a maximum sentence of 20 years in prison. The fourth count charges the making of false statements to the FBI, which carries a maximum sentence of five years in prison. The maximum potential sentences are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendant will be determined by the judge.

Mr. Williams praised the extraordinary work of the FBI.

This case is being handled by the Office's Complex Frauds and Cybercrime Unit. Assistant U.S. Attorney Vladislav Vainberg is in charge of the prosecution.

The charges contained in the Indictment are merely accusations, and the defendant is presumed innocent unless and until proven guilty.

---

[1] As the introductory phrase signifies, the entirety of the text of the Indictment, and the description of the Indictment set forth herein, constitute only allegations, and every fact described should be treated as an allegation.

Attachment(s):
Download nickolas_sharp_indictment_redacted.pdf

Topic(s):
Financial Fraud

Component(s):
USAO - New York, Southern

Contact:
Nicholas Biase, James Margolin
(212) 637-2600

Press Release Number:
21-341

Updated December 1, 2021